

Application No. 09/882,185
Response to Final Office Action

Customer No. 01933

R E M A R K S

Reconsideration of this application is respectfully requested.

According to the present invention as recited in independent claims 16-18, a ciphering apparatus, method, and computer program are provided which divides plaintext into blocks, and then divides at least one of the blocks into sub-blocks. As recited in independent claims 16-18, a ciphering attribute is set for each of the blocks for use in ciphering, and a sub ciphering attribute is set for each of the sub-blocks for use in ciphering. And as recited in independent claims 16-18, the data of each of the sub-blocks is ciphered in accordance with the corresponding set sub ciphering attribute, and the at least one block that includes the ciphered data of the sub-blocks is ciphered in accordance with the set ciphering attribute corresponding to the block.

With this structure, attribute hierarchy can be achieved, so as to allow effective security management.

The Examiner contends that USP 6,307,940 ("Yamamoto et al") discloses dividing plaintext into blocks and setting a ciphering attribute for each of the blocks, as well as dividing at least one of the blocks into sub-blocks and setting a sub ciphering attribute for each of the sub-blocks. As support for these

Application No. 09/882,185
Response to Final Office Action

Customer No. 01933

assertions, the Examiner points to the disclosure at column 18, lines 29-47 and 58-64 and column 19, line 40 to column 20, line 67 of Yamamoto et al.

It is respectfully submitted, however, that Yamamoto et al merely discloses dividing plaintext into blocks, and ciphering groups of the blocks with a same key. In Yamamoto et al, in order to keep the ciphering system safe, a key is only used for "s" number of blocks before the key is changed. Therefore, according to Yamamoto et al, a first "s" number of blocks of plaintext are ciphered using a key k_1 , and then a second "s" number of blocks are ciphered using a next key k_2 . See Yamamoto et al at column 20, lines 12-15.

In the example given at column 18, lines 58-64 of Yamamoto et al, which was cited by the Examiner, if there are 15 blocks of plaintext and the number "s" is 10 (see column 18, lines 36-39), then the first 10 blocks are ciphered with a first key k_1 , and the next 5 blocks are ciphered with the next key k_2 .

Thus, if the Examiner is interpreting the groups of "s" number of blocks of plaintext of Yamamoto et al to be the "blocks" of the claimed present invention, and the individual blocks of plaintext of Yamamoto et al to be sub-blocks, then Yamamoto et al only discloses setting ciphering attributes (keys k_1 and k_2 , etc.) for the blocks.

Application No. 09/882,185
Response to Final Office Action

Customer No. 01933

That is, using the Examiner's interpretation of Yamamoto et al, it is respectfully submitted that Yamamoto et al does not disclose, teach or suggest a sub-block attribute setting section which sets a sub ciphering attribute for each of the sub-blocks for use in ciphering, in the manner of the claimed present invention. In this connection, it is respectfully pointed out that the Examiner has cited the same keys k_1 and k_2 as being both the ciphering attributes and the sub ciphering attributes of the claimed present invention.

Indeed, the Examiner acknowledges on page 3 of the Office Action that Yamamoto et al does not disclose, teach or suggest a block ciphering section which ciphers the at least one block that includes the ciphered data of the sub-blocks in accordance with the ciphering attribute corresponding to the block set by the block attribute setting section. For this reason, the Examiner has cited USP 5,588,075 ("Chiba et al") to supply the missing teachings of Yamamoto et al.

It is respectfully submitted, however, that Chiba et al also does not disclose, teach or suggest a block ciphering section as according to the present invention as recited in claim 16, or the corresponding steps of claims 17 and 18.

The Examiner argues that Chiba et al discloses dividing image data into a number of blocks and allocating the number of

Application No. 09/882,185
Response to Final Office Action

Customer No. 01933

blocks into a macro-block, and that the block is encoded before it is allocated into a macro-block, which is then encoded.

It is respectfully submitted, however, that Chiba et al merely discloses dividing an image into blocks of 8x8 pixels. The blocks are compared to previous frame images to determine whether each block is an "effective block" that has changed at least by a threshold amount with respect to the previous frame image. The 8x8 pixel blocks are then defined as part of macro blocks, and the macro blocks are encoded by JPEG. The encoding order of the macro blocks may be based on the determinations of effective blocks of pixels. (See Chiba et al at column 6, lines 30-65, cited by the Examiner.) Once a macro block has been encoded, it is transmitted to a decoding side. In Chiba et al, the order of encoding of the macro blocks is significant because only a certain amount of encoded information can be transmitted per frame. Thus, the recognition of effective blocks can ensure that the portions of the image that are changing in a given frame are transmitted. (See, for example, Chiba et al at column 10, lines 40-60, cited by the Examiner.)

It is respectfully submitted that the 8x8 pixel blocks of Chiba et al are merely analyzed to determine whether they have changed with respect to the same blocks in a previous frame, and the macro blocks made up of the 8x8 pixel blocks may be encoded

Application No. 09/882,185
Response to Final Office Action

Customer No. 01933

based on the frequency of effective blocks within the macro blocks.

It is respectfully submitted that Chiba et al does not disclose, teach or even remotely suggest that the 8x8 pixel blocks are first encoded (with a sub ciphering attribute), and that the macro blocks are then encoded (with a ciphering attribute), in the manner of the claimed present invention.

Accordingly, it is respectfully submitted that even if the teachings of Yamamoto et al and Chiba et al were combinable in the manner suggested by the Examiner, such combination would still not achieve or render obvious the features of the present invention as recited in independent claims 16-18.

In view of the foregoing, it is respectfully submitted that the present invention as recited in independent claims 16-18 clearly patentably distinguishes over the combination of Yamamoto et al and Chiba et al under 35 USC 103.

* * * * *

Allowance of the claims and the passing of this application to issue are respectfully solicited.

Application No. 09/882,185
Response to Final Office Action

Customer No. 01933

If the Examiner has any comments, questions, objections or recommendations, the Examiner is invited to telephone the undersigned at the telephone number given below for prompt action.

Respectfully submitted,

/Douglas Holtz/

Douglas Holtz
Reg. No. 33,902

Frishauf, Holtz, Goodman & Chick, P.C.
220 Fifth Avenue - 16th Floor
New York, New York 10001-7708
Tel. No. (212) 319-4900
Fax No. (212) 319-5101

DH:iv